Project: State of Washington Multi-Agency Forest Project

Title: **Windows 2000 Security Plan**

Version: 1.0

Status: Approved

Date: October 11, 2001

State of Washington
Windows 2000 State Forest

Windows 2000 Security Plan

Document Information

Title	Windows 2000 Security Plan
Status	In Development
Authors:	Anthony Witecki, Microsoft Consulting Services John Ditto, Dept of Information Systems
Reviewers:	Forest Resource Group, Steering Committee

Document History

WHEN	WHO	WHAT
7/30/01	Anthony Witecki	Initial document draft. Has not been reviewed by Security Sub-Group or Forest Resource Group.
8/30/01	Anthony Witecki	Initial document draft. Has been reviewed by Security Sub-Group and Forest Resource Group.
9/05/01	John Ditto	Entered into the Document Approval Process as Draft for Comment.
9/27/01	John Ditto	Edited to add Policy Summary.
10/11/01	John Ditto	Edited to include Password Security Policy

Table of Contents

Executive Summary

About Security

Security is an important part of system infrastructure. An information system with a weak security foundation will eventually experience a security breach. Examples of security breaches include data loss, data disclosure, loss of system availability, corruption of data, and so forth.

The primary goals of the security infrastructure are:

1. **Data Confidentiality** – only authorized users should be able to use data in the Windows 2000 forest environment.
2. **Data Integrity** – users should feel confident that the data, information and knowledge they are using is accurate and has not been modified in transit.
3. **Data Availability** – users should be able to access the data they required when they need it.

These goals are important to the design and implementation of security policies. For example, any security policy that prohibits users from accessing information they need is effectively worthless. Likewise, if security policies are too lax, users will not have the confidence that the information they are using is accurate or relevant.

Policy

Policy as referred to in this document is organized and listed specifically for each asset identified. Each is based on the assessment of threats, vulnerabilities, available safeguards, and constraints. The following security policies are to be implemented on the State of Washington Windows 2000 Forest.

Root Hardware

- All Root hardware is to be stored in locked storage cabinets at the DIS data center.
- Only enterprise administrators and necessary support staff have physical access to the root hardware.

DNS Topology and Zone Transfer

- All DNS Servers in the Windows 2000 Forest will run on Domain Controllers and take advantage of Active Directory – integrated DNS functionality.
- All Domain Controllers in the Windows 2000 Forest will communicate with each other using IPSec
- All Agency-level DNS servers must be configured to use the WA.LCL forest root DNS servers as forwarders. Recursion should be disabled on all internal DNS servers.
- The root directory will assign all IP addresses manually. DNS resource records will be entered at creation and Windows 2000 Access Control Lists will be used to allow only root administrators to make changes to zone data.
- Dynamic DNS will be disabled in the Forest Root, as will DHCP.
- All domain controllers must be logically located inside the DIS Internet firewall.

WINS Database

- All WINS Databases must be backed up locally and to removable media at least once per day.
- WINS servers must take advantage of IPSec communications when replicating with other WINS servers.

Active Directory Global Catalog Data

- The root domain will provided a minimum of two global catalog servers for redundancy and replication load balancing.
- Each agency requesting a domain in the forest will be required to provide and maintain at least one global catalog server and one domain controller. Small agencies combining resources under a single umbrella domain will need a minimum of one domain controller and one global catalog for the entire umbrella domain.
- System State Data, which includes the global catalog database, will be backed up on a daily basis and historical, rotated backups will be maintained for a period of six months.
- By default, all objects and their associated attributes will be owned by the system administrators in the domain to which they belong. Any organization or group that requires ownership of an attribute must request ownership through the formal change management process.
- The State-wide Forest Steering Committee will assign the task of defining attribute usage for various objects stored in global catalogs to ensure consistency among agencies.

Active Directory Replication Traffic

- All domain controllers will be configured for IPSec to ensure encrypted communication at all times among domain controllers and global catalogs in the forest.
- DIS will provide a minimum of two root redundant bridgehead servers (configured as Global Catalogs) for ensuring that replication between the hub and any agency spoke is available at least once during every 24 hour period.
- Replication will be monitored on a daily basis by Forest Operations personnel. Incomplete or failed replication attempts will be escalated as appropriate. Overall replication traffic will also be measured on a regular basis to anticipate and handle issues related to performance and capacity planning.
- Security settings that must be applied forest wide through group policy will be replicated manually, initiated through the NTDS replication process.
- The knowledge consistency checker will be turned off for inter-site replication after an Agency has successfully joined the forest. This prevents unauthorized replication connectors from being created.

Active Directory FSMO Roles

- Operation master roles must be properly transferred to another server before demoting or otherwise removing the hosting domain controller or global catalog from the domain.
- In the event of unanticipated failure by a FSMO role, the role will be seized by another valid domain controller or global catalog until the original machine can be brought back up online.

Active Directory Configuration Container

- Access to objects in the Active Directory configuration container will be restricted to members of the enterprise administrators group. Changes to permissions, creation of additional objects, and deletions of objects will be conducted only through formal procedures that are supported by Microsoft Product Support Services.

Active Directory Schema

- The Active Directory Schema is owned and maintained by the Enterprise Schema Administrators group. All changes to the Schema must be submitted through the change management process with a valid business justification and approved by the Forest Resource Group and Forest Steering Committee.

Authentication – Domain Administrators

- All Domain Administration Account login IDs must be authorized and approved.
- All Domain Administrator accounts are to be used for administration purposes only. Each Administrator will have a normal user account for day-to-day office work.
- All Domain Administration Account login IDs must have a complex password of at least 8 characters. Complexity is defined as having at least three of the following four types of characters: lower case letters, upper case letters, numbers, or special character.
- Login IDs are not to be shared.
- Only the owner of a password is to know that password.
- Passwords must be changed every 90 days. Passwords cannot be changed for at least 7 days after the initial change (minimum password change length).
- System lockout will take effect for 30 minutes if more than 5 bad login attempts are made within a 30 minute period.
- Password history is maintained for 18 iterations, ensuring that the same password is not re-used at least 18 times.

Authentication – Users

- Must follow ISB Recommendations for General Access Security

Authorization (Access Controls)

- Groups are used to manage permissions to all Active Directory Objects, including file shares and printers.
- Use Secure Dynamic Updates for Dynamic DNS entries.
- Use Organizational Units to group users and administrators, applying the appropriate policies to each.
- Set permissions compatible with Windows 2000 Only (non mixed-mode).
- Domain controllers are physically secured

Audit

- Each agency must define and maintain an intrusion detection policy. At a minimum, intrusion detection should regularly monitor failed login attempts.
- Changes made to the security policy of a domain must be audited.

Backup and Recovery

- Each agency is responsible for maintaining at least two iterations of validated backup information for the active directory data in

their domain (to ensure recoverability of the state-wide global catalog)[1].

The media for validated domain backups must allow a recovery history of at least 30 days and must be stored off-site.

All backup media, on and off-site, must be securely stored.

How to Use This Document

This document was developed by identifying the forest-wide resources requiring protection. For each asset, an assessment of the related threats, vulnerabilities, and constraints was performed to provide a basis for policies and related control activities that would enhance the security of those objects.

Risk Assessment

Risk is the probability that a threat agent (cause) will exploit a system vulnerability (weakness) and thereby create an effect detrimental to the system.[1] Risk assessment begins with an analysis of the inherent risk in an environment. It concludes with an assessment of present risk and residual risk. Present risk is the assessment with existing safeguards taken into account. Residual risk considers existing safeguards, as well as, planned or recommended safeguards. Risk assessment deals with the following elements:

1. Identification of Assets
2. Threats
3. Vulnerabilities
4. Safeguards
5. Constraints

Identification of Assets

This section attempts to answer the question, "What assets are at risk?" as it relates to the Windows 2000 environment. This document deals specifically with the root and Forest-wide issues only. Individual agency domains will likely identify similar or complimentary assets.

The question "What assets are at risk?" is an attempt to identify what, in the Windows 2000 environment, is likely to be the subject of a security breach. Subsequent sections will deal with the threats, sources and severity of such risks.

The table on Page 17 outlines the assets that have been identified in the root domain and forest-wide. Individual agencies should recognize these objects as well as agency-specific resources in their own security plans.

[1] Two iterations and 30 days of history are a minimum. The purpose behind multiple iterations is to allow for the possibility that the most recent backup information is corrupt or invalid. The purpose behind the 30 day minimum is to ensure that the state can recover from any problem that may have been discovered during the past month.

The value of each asset is also identified either for its cost or importance to the State of Washington. Most forest root assets have a higher value in a connected system than they would stand-alone, so any dependencies have also been identified.

Irrespective of their value to an organization, some assets are more prone to loss than others. This is referred to as asset exposure and is used to justify additional spending for safeguards protecting the asset.

Threats

A threat is a possible source of danger to an IT system. A threat agent can be a person or phenomenon that can make a threat manifest. Threats include, but are not limited to, natural disasters, shortages of essential services, equipment malfunctions, theft, fraud or trespass.[2]

Threats can be accidental or deliberate. To realize a deliberate threat, the perpetrator must have **capability, motivation, and opportunity**. Accidental threats are events, actions or omissions that are not directed at a specific system and caused by a human or natural threat agent. Accidental threats include fires, software failures, hardware failures, earthquakes, and operator errors. The table on page 35 identifies general threats that exist in the root domain and enterprise-wide Windows 2000 forest. A more detailed list of threats exists in each of the subsequent control sections.

Risk assessment involves the identification of threats and their likelihood (as well as frequency), severity, and consequence. Expectancy can be evaluated mathematically or qualitatively, but should be adequate to justify the cost of protecting an asset from the identified threat.

Vulnerabilities

A vulnerability is any system weakness that can be exploited by a threat agent. Weaknesses can be either systemic or temporary lapses.[3] Vulnerabilities are different from threats in that they sometimes provide the opportunity for a threat agent to act against an asset. Vulnerabilities are identified for each corresponding asset protected in this document.

Safeguards

Safeguards are either checks or restraints imposed on a system to enhance security.[4] Safeguards work in any of the following ways:

1. Prevent Risk – typically involves strengthening the security environment.
2. Transfer Risk – used mostly for financial risk and typically involves insurance policies, warranties or contracts.
3. Reduce Likelihood – typically enforced by policy, this ensures that risks are less likely to happen, but does not represent a technical solution as prevention does.
4. Reduce Vulnerability – this involves system hardening not specific to the security infrastructure. RAID subsystems are a

good example where the vulnerability of a single disk failure is reduced.

5. Mitigate Impact – used primarily after-the-fact to restore operations quickly.
6. Detective Controls – use system auditing capabilities to detect suspicious activities and act quickly.

Safeguards ultimately become part of the policies and procedures for security implementation and are defined in subsequent sections of this document.

Constraints

Constraints are system requirements that affect the selection of a safeguard to protect an asset from a threat. Constraints can be financial, time, technical, legal, environmental and sociological.

Time constraints are minimal in the State of Washington for security planning purposes. Because we have chosen an in-place migration plan for Windows 2000, safeguards can be implemented as systems and users are moved over.

Financial constraints are considerably more serious. Because the State of Washington operates on a biennium basis, the cost of safeguards must be taken into consideration at the beginning of the budgetary process to avoid the need for emergency funds.

Technical constraints will be limited primarily by hardware chosen at the root and agency levels. In accordance with the Root Health Monitoring document, the root has ample hard drive space, memory and processor to implement, analyze and control the Windows 2000 Security environment. Technical constraints will be most prominent for environments that make heavy use of security auditing or performance analysis.

Sociological constraints are likely to be a problem in the State of Washington. Some people are uncomfortable with security or believe that security safeguards infringe on their "rights." Dealing with sociological constraints will require cooperation with the Department of Personnel.

Environmental constraints are generally avoidable, but because the majority of the State of Washington's operations facilities lie on an earthquake fault line, it is impossible to ignore the impact such an event might have.

The State of Washington is subject to legal constraints as outlined in the Revised Code of Washington and the Washington Administrative Code. Such constraints must be considered when evaluating safeguards against certain threat agents.

Asset: Root Hardware

Description: The root hardware is limited to the physical machines supported by the forest enterprise administrators.

Dependencies, Exposure and Value

The hardware investment is the single most important component of the security plan, given that all forest-wide dependencies ultimately rely on it. However, its exposure is limited to administrative personnel with access to the DIS data center.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Hardware component failure.	Accidental	Depending on the component, this could be as minimal as decreased performance to complete unavailability.	Moderate
Total hardware failure.	Accidental	Potential unavailability of network services. All machines configured to use a specific server for a network function would experience total outage for that service.	Low
Unauthorized change	Internal	Most changes made to hardware would be done so with good intentions. However, the failure to properly implement these changes or notify those impacted could result in a loss of some network services.	Low
Theft	Internal (External)	Depending on the components taken, impact ranges from loss of performance all the way through loss of availability.	Low

Vulnerabilities

Vulnerability	Impact
All hardware is subject to a metric known as the Mean Time Between Failure (MTBF), which is the average life of the hardware.	Ranges from temporary performance problems (in the event of a lost hard drive) to complete system unavailability (RAM failure). Impact is easily mitigated by regularly replacing aging hardware.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in

conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
DIS maintains all root hardware in locked storage cabinets in the DIS central data center.	Only enterprise administrators, trained on Windows 2000 and familiar with the environment and change control process have access to the hardware.

Constraints

No constraints have been identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

Forest-wide hardware resources shall be protected from failure at both the system and individual component levels.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
1. All Root hardware is to be stored in locked storage cabinets at the DIS data center.	not applicable
2. Only enterprise administrators and necessary support staff have physical access to the root hardware.	not applicable

Asset: DNS Topology and Zone Transfer

Description: Active Directory uses the Domain Name System for name resolution, to locate services, and to establish the domain namespace for the Active Directory hierarchy. DNS affects the design of the organizational layout including forests, trees, domains, and sites.[5]

Dependencies, Exposure and Value

DNS represents the foundation of Windows 2000 Active Directory. Nearly all active directory services, as well as client and server name resolution depend on DNS to establish communication in a distributed environment. For that reason, the value of DNS is extremely high and requires careful consideration during security planning. In addition, the DNS service has high visibility and exposure, being based on open standards that were originally conceived for public networks with minimal security considerations. Windows 2000's implementation of DNS extends the RFC by adding Windows-specific security options.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Improperly secured DNS Servers.	External Agents Deliberate.	If the server records are exposed, external attackers will be able to completely map the internal network by querying the DNS server.[6] This information would most likely be used to launch denial of service attacks against specific resources or used to identify machines likely to contain sensitive data.	Medium to Low
Unauthorized changes to DNS records.	Operator Users External Agent Accidental or Deliberate.	If resource records (RRs) are changed, or if the underlying IP addresses of servers change and RRs are not updated to reflect the change, service outages or configuration problems can occur.	High to Medium
Resource Records Contain Server Functions.	Internal or External Agents Deliberate	Identification of machines by function can provide malicious users with information that would be helpful in the compromise of sensitive information. At particular risk are database and application resources.	Medium to Low

Vulnerabilities

The following vulnerabilities exist in the State of Washington's implementation of Windows 2000.

Vulnerability	Impact
DHCP Server, running on a domain controller, can compromise secure dynamic updates if configured to register DNS records on behalf of clients.	The impact is minimal in the root domain, as DHCP is not used. However, it may cause problems in client domains that have a small impact on the overall forest health.
DNS traffic travels through port 53 (UDP and TCP).	Agencies using firewalls that do not enable active directory zones must open port 53 for TCP and UDP. Traffic should only be allowed from the inside out.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Active Directory integrated zones allow access control over who can update DNS and provide better replication and fault tolerance capability.[7]	This prevents unauthorized changes and insecure zone transfers. It preserves the integrity of zone data.
Specify DNS administrators groups and users specifically to manage DNS and configure ACLs on DNS Zones.	Prevents risk by limiting access to zone information to only authorized users. Preserves integrity of data.
Create an enterprise DNS audit policy; use Active Directory DNS interface to log and monitor DNS events.	This detects problems or attempts at unauthorized access to zone information.
Use more than one DNS server to host each zone, for fault tolerance.	This mitigates the risk that DNS information will be unavailable.
Windows 2000 provides the ability to control zone transfers.	Since zone transfers move all the records for a particular zone from one server to another it is extremely important not to transfer the forward lookup zone on a DNS server that contains Windows 2000 domain information to any server outside the Windows 2000 domain.
IPSec can be enabled between domain controllers to secure the transmission of Active Directory replication information, including Zone transfers.	This provides authentication of both the sending and receiving machines and secures the transmission of information using a shared secret key that exists only during the life of the session. It prevents risk and contributes to the integrity and confidentiality of transferred DNS information.
All Windows 2000 Machines can be located behind the DIS public firewall.	This reduces the likelihood of an external attack, but does not necessarily prevent problems from internal threats. It contributes primarily to the confidentiality of DNS information from outsiders.

Constraints

No constraints have been identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

Forest-wide DNS resources are to be protected against unauthorized access, unauthorized changes and unintentional disclosure. The following control procedures address the security of zone database files stored locally, accessible via DNS query, and transferred during zone transfers.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
1. All DNS Servers in the Windows 2000 Forest will run on Domain Controllers and take advantage of Active Directory – integrated DNS functionality.	Follow instructions documented in the Forest Root Requirements Document.
2. All Domain Controllers in the Windows 2000 Forest will communicate with each other using IPSec.	Follow instructions documented in the Forest Root Requirements Document.
3. All Agency-level DNS servers must be configured to use the WA.LCL forest root DNS servers as forwarders. Recursion should be disabled on all internal DNS servers.	1. Open DNS Manager from the Administrative Tools folder. 2. Right-click the server name of the server you wish to configure and select Properties. 3. On the Forwarders tab, enter the IP address of at least 2 DNS servers in the WA.GOV public name space. 4. Be sure that the Disable Recursion check box is turned ON and click okay. 5. Stop and Restart the DNS Service from the Services console under administrative tools.
4. The root directory will assign all IP addresses manually. DNS resource records will be entered at creation and Windows 2000 Access Control Lists will be used to allow only root administrators to make changes to zone data.	Follow instructions documented in the Forest Root Requirements Document.
5. Dynamic DNS will be disabled in the Forest Root, as will DHCP.	Follow instructions documented in the Forest Root Requirements Document.
6. All domain controllers must be logically located inside the DIS Internet firewall.	Use IP addresses for internal IP scopes on all domain controller machines.

Asset: WINS Database

Description: WINS is the name resolution system used for Windows NT Server 4.0 and earlier operating systems. WINS uses flat NetBIOS naming conventions and provides an important service for network administrators with heterogeneous systems supporting clients running older operating systems, such as Windows 95 and Windows NT 4.0. These older systems do support DNS name resolution but do not support dynamic updates to DNS records.

Dependencies, Exposure and Value

Although WINS support is important during the migration process and for purposes of maintaining legacy client name resolution, its overall value is relatively low. The long-term plan involves replacing WINS with Dynamic DNS. WINS has little or no exposure in terms of a threat target, but does have a history of problems that might lead to unavailability or related problems.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Loss of WINS database information.	Software Failures or Operator Error	Legacy clients and applications that require WINS for distributed computing may not be able to communicate during the outage.	Moderate
Corruption of WINS Database.	Software Failures or Operator Error	Name resolution works improperly, disrupting communications. May be difficult to detect.	Moderate
Loss of Access to WINS database.	Hardware Failure or Operator Error	Minimal. Up to 12 WINS servers can be configured and operating for redundancy.	Low
Compromise of internal namespace.	External Trespass or Operator Error	Exposing the IP addresses and names of servers potentially provides a road map to network attackers.	Low

Vulnerabilities

The following vulnerabilities exist in the State of Washington's implementation of Windows 2000.

Vulnerability	Impact
WINS requires considerable planning and setup to properly work within an organization. This is often overlooked because of its seemingly simple design.	Availability and functionality can be affected if WINS is not properly implemented in an environment. Improper planning may also cause overall availability or performance problems, particularly related to network and wide area traffic.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Windows 2000 allows up to 12 WINS servers to be available to clients.	This provides considerably more redundancy and availability than what was possible in earlier versions of Windows Servers.

Constraints

No constraints were identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

The WINS databases, owned and maintained by individual agencies, must be protected against loss of use and loss of confidentiality.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
All WINS Databases must be backed up locally and to removable media at least once per day.	1. Open WINS. 2. In the console tree, click the applicable WINS server. 3. On the Action menu, click Backup Database. Do not specify a network drive as the backup location. 4. When prompted to confirm, click Yes. After backup is completed, click OK. **NOTE:** if you change the WINS backup or database path in server properties, perform new backups to ensure successful future restorations of the WINS database.
WINS servers must take advantage of IPSec communications when replicating with other WINS servers.	See Forest Root Requirement Document for information about setting up IPSec in the Windows 2000 environment.

Asset: Active Directory Global Catalog Data

Description: The Global Catalog is a complete list of all objects in the Active Directory environment. Every object is instantiated from an object class and is described by a series of object attributes. Object attribute data must be available to legitimate users, hidden from unauthorized users, and protected from change, except by appropriate state personnel. In addition, the extension of global catalog data must be limited to authorized personnel for changes, additions or deletions.

Whereas domain controllers contain a complete set of attributes for the objects they contain, global catalogs contain only a partial list, facilitating replication and increasing query speeds. As such, it is necessary to protect both the global catalogs as assets, as well as the domain controllers themselves, which contain the complete set of attributes for every object within their domains.

Dependencies, Exposure and Value

The global catalog provides the fundamental structure and organizational architecture for people and technical resources in the Windows 2000 environment. For that reason, nearly every enterprise resource or application ultimately depends on the global catalog availability in one way or another. The GC itself, however, depends only on the Windows 2000 systems architecture.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Unauthorized changes to AD object attribute data.	Internal Deliberate or Accidental	Depending on the attribute changed, this could result in very minor misinformation problems all the way through application availability problems (in situations where applications look for specific attributes to determine how they function).	Deliberate is Low, but Accidental is more likely during the initial phases of the rollout.
Global Catalogs not available for processing logon requests.	Technical Accidental	Minimal. Users can be authenticated without the presence of a global catalog, but their group membership tokens from other domains in the forest would not be properly loaded.	Low in larger agencies. High in small agencies.

Vulnerabilities

Vulnerability	Impact
Line of Business Applications that are built in the Active Directory Forest and make updates to Global Catalog data represent a potential opportunity to corrupt data.	Depending on the scope and quality assurance of the development process, the LOB application may make changes to AD data that render the data useless to other applications reading the changed attribute.

Lack of training for professionals making updates to AD global catalog data.	Unfamiliarity with the prescribed attribute definitions may cause inconsistencies among agencies as to the values placed in various attribute fields.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Global Catalogs can be created quickly and easily by simply making any domain controller a global catalog. If all GCs were simultaneously lost, they could be created through normal replication of existing domain controllers.	This prevents global catalog data from being unavailable for extended periods of time. However, it is dependent on the availability of domain controllers for each domain in the forest.
Active directory allows for partitioning of global catalog data through the implementation of domains.	This prevents the loss of data in one agency from directly impacting the resources of another. It does not, however, prevent bad data in one agency from replicating to another.
Redundant domain controllers reduce the likelihood of loss from a single server failure.	Preserves the AD environment in the event of a hardware failure. Geographic isolation prevents failure in the event of large scale disaster.

Constraints

No constraints were identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

The data collected, stored, and replicated in the State of Washington's global catalog must be protected against unauthorized changes and loss of use due to hardware failures or network service outages.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
The root domain will provided a minimum of two global catalog servers for redundancy and replication load balancing.	See the "Root Domain Requirements" document for implementation details.
Each agency requesting a domain in the forest will be required to provide and	Not applicable.

maintain at least one global catalog server and one domain controller. Small agencies combining resources under a single umbrella domain will need a minimum of one domain controller and one global catalog for the entire umbrella domain.	
System State Data, which includes the global catalog database, will be backed up on a daily basis and historical, rotated backups will be maintained for a period of six months.	Backup procedures and verification are identified in the Forest Root Requirements Document.
By default, all objects and their associated attributes will be owned by the system administrators in the domain to which they belong. Any organization or group that requires ownership of an attribute must request ownership through the formal change management process.	Not applicable.
The State-wide Forest Steering Committee will assign the task of defining attribute usage for various objects stored in global catalogs to ensure consistency among agencies.	Not applicable.

Asset: Active Directory Replication Traffic

Description: Replication takes two forms. Within a domain, replication occurs between all domain controllers in that domain. Within a forest, replication takes place for a subset of all object attributes (known as the global catalog) across domain boundaries. Replication also uses several transports, depending on the connectivity between the participating machines. Machines within the same site are updated continuously through RPC calls. Machines in separate sites, however, are updated using compression on a scheduled basis over IP or SMTP.

Dependencies, Exposure and Value

Replication is the process which exposes the data contained in Active Directory to the wire. Without any controls in place, anyone with a network protocol analyzer could gain access to the information stored in Active Directory. Exposure for this asset is high, given that it travels throughout the forest across potentially insecure wires.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Compromise of Active Directory Data through protocol analysis.	Internal or External Deliberate	Unauthorized users would have information about the state-wide user directory and network topology that could be used for denial of service attacks, social engineering, or other targeted attacks.	Moderate
Replication Failure.	Technical or Administrator Accidental	Users and applications in remote domains would not have access to changes made since the last successful replication process. The impact can be more serious in situations where security settings for users or machines must be immediately applied forest-wide. Such situations may expose other resources on the network if group policies cannot be enforced in a timely manner.	Moderate

Vulnerabilities

The following vulnerabilities exist in the State of Washington's implementation of Windows 2000.

Vulnerability	Impact
Active Directory replication depends on DNS to function properly.	If AD is dependent on an insecure or improperly configured DNS platform, replication is more likely to fail. Impact would be minimal provided DNS records could be quickly reconstructed to their proper values.
By design, Active Directory handles certain	Inefficient changes can cause increased replication

environmental changes more efficiently than others.	traffic that deny other forest services or increase the latency between multiple agencies in the forest. The impact is only relevant in environments where lack of bandwidth is a security concern.
Replication in Active Directory is dependent on Kerberos for authentication, which requires that all domain controllers be time-synchronized.	Machines where respective clocks are off by more than 5 minutes fail to authenticate properly with one another and cannot securely timestamp replication attempts, preventing replication from occurring.

Security Safeguards

The following safeguards can be implemented to reduce overall risk.
The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Windows 2000 provides out-of-box support for IPSec.	IPSec secures communication between any two computers by ensuring each computer properly authenticates itself and encrypts every packet exchanged during the session. IPSec uses public-private key-pairs for authentication, as well as secret session keys to ensure privacy.
Active Directory-Integrated DNS Service is supported out-of-box to provide security of DNS resource records.	Controlling change over DNS records ensures that unauthorized changes that might interrupt network communications do no occur. This reduces the likelihood that replications will be uninitiated.
The NET TIME command can be used on a scheduled basis to ensure that system clocks are properly synchronized.	The use of this command prevents system clocks from getting out of sync with one another.

Constraints

No constraints were identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

Replication of global catalog and domain controller traffic will be kept confidential within the State of Washington Windows 2000 administrators.
Replication will occur at regular intervals such that all child domains in the Active Directory forest are synchronized with the root at least once during every 24 hour period.
All domain controllers will synchronize their system clocks with the root to ensure that Kerberos properly authenticates machines and allows for the digital signing of replication traffic.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
All domain controllers will be configured for IPSec to ensure encrypted communication at all times among domain controllers and global catalogs in the forest.	See "Root Requirements Document" for information on configuring IPSec for domain controllers.
DIS will provide a minimum of two root redundant bridgehead servers (configured as Global Catalogs) for ensuring that replication between the hub and any agency spoke is available at least once during every 24 hour period.	Setup for these two machines are defined in the root requirements document.
Replication will be monitored on a daily basis by Forest Operations personnel. Incomplete or failed replication attempts will be escalated as appropriate. Overall replication traffic will also be measured on a regular basis to anticipate and handle issues related to performance and capacity planning.	See "Root Health Monitoring Document" for specific details.
Security settings that must be applied forest wide through group policy will be replicated manually, initiated through the NTDS replication process.	1. Open Active Directory Sites and Services. 2. In the console tree, double-click the domain controller for the site containing the connection over which you want to replicate directory information. 3. In the console tree, click NTDS Settings. 4. In the details pane, right-click the connection over which you want to replicate directory information, and then click Replicate Now.
The knowledge consistency checker will be turned off for inter-site replication after an Agency has successfully joined the forest. This prevents unauthorized replication connectors from being created.	See "Root Requirements Document" for details about turning off the KCC.

Asset: Active Directory FSMO Roles

Description: Certain domain and enterprise-wide operations not well suited to multi-master placement reside on a single domain controller in the domain or forest. The advantage of single-master operation is to prevent the introduction of conflicts while an operation master is offline, rather than introducing potential conflicts and having to resolve them later.

The Active Directory defines five FSMO roles: schema master, domain master, RID master, PDC emulator, and infrastructure. The schema master and domain naming master are per-forest roles. The remaining three, RID master, PDC emulator, and infrastructure master, are per-domain roles.

Dependencies, Exposure and Value

Because only one server per domain or forest is appointed to serve as each of the respective FSMO roles, such services are subject to a single point of failure. Although they contain information important to the infrastructure of the domain and forest, FSMO roles have not been the targets of internal or external threats and have relatively low exposure compared with other domain and forest services.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Unavailability of FSMO Role, including Denial of Service Attacks.	Technical, Operator or External Deliberate or Accidental	The unavailability of some FSMO roles may prevent domain or forest operations from occurring, such as creating new users, computer accounts, or infrastructure components.	Low

Vulnerabilities

The following vulnerabilities exist in the State of Washington's implementation of Windows 2000.

Vulnerability	Impact
By definition, FSMO roles represent a short-term single point of failure.	The impact of this vulnerability is limited to the time it would take to transfer or seize the role, moving it to another machine, or brining the original machine back online. Overall, short-term failures represent minimal impact to the overall environment.
Infrastructure Master does not properly update when installed on a Global Catalog.	Infrastructure information is not replicated using the normal replication process. Q248047 describes, in detail, how the replication works and why it fails to work on a global catalog server. The impact is outdated or incorrect data hosted on the Infrastructure Master machine.

Schema and Domain Naming Masters may not function properly when not installed on a global catalog.	Without access to global catalog data, the domain naming master may not be able to properly verify the name of a new object. Without it, domains cannot be added or removed.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Microsoft provides tools with Windows 2000 to manually transfer or seize FSMO roles to available domain controllers.	These tools, used in conjunction with early detection, can ensure that FSMO servers are always available to process changes, additions, and deletions of the forest objects.

Constraints

No constraints were identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

The physical location (server name) of all FSMO roles in the root domain will be documented in the root domain requirements. The schema master and domain naming master will reside on a global catalog server. The infrastructure master will run on a domain controller that is NOT a global catalog server in the same physical site as a root global catalog server.

Servers that host FSMO roles will have redundant hardware and be monitored 24X7 by DIS operations staff.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
Operation master roles must be properly transferred to another server before demoting or otherwise removing the hosting domain controller or global catalog from the domain.	1. Open Active Directory Schema. 2. In the console tree, right-click Active Directory Schema and then click Change Domain Controller. 3. Click Any DC to let Active Directory select the new schema operations

	master. 4. Or, click Specify Nameand type the name of the new schema master computer. 5. In the console tree, right-click Active Directory Schema, and then click Operations Master. 6. Click Change.
In the event of unanticipated failure by a FSMO role, the role will be seized by another valid domain controller or global catalog until the original machine can be brought back up online.	1. Click Start, click Run, and then type **cmd**. 2. At the command prompt, type **ntdsutil**. 3. At the ntdsutil prompt, type **roles**. 4. At the fsmo maintenance prompt, type **connections**. 5. At the server connections prompt, type **connect to server**, followed by the fully qualified domain name. 6. At the server connections prompt, type **quit**. 7. At the fsmo maintenance prompt, type **seize <name of FSMO role>**. 8. At the fsmo maintenance prompt, type **quit**. 9. At the ntdsutil prompt, type **quit**.

Asset: Active Directory Configuration Container

Description: Active Directory stores information about the physical network in the Configuration container and uses it to guide the creation of replication connections between domain controllers. Directory-aware applications store information in the Configuration container that applies forest wide.

Dependencies, Exposure and Value

The configuration naming context (container) holds information about the physical site layout, the structure of trees in the forest, and the global configuration information for services. Further, Active Directory-aware applications store information in the Configuration directory partition. It exists only in the root domain and is replicated to all GCs in the forest. As a result, its value is high and several Windows 2000 services, including replication, depend on it.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Improper modification of configuration objects.	Internal Accidental or Deliberate	Impact ranges from minor inconveniences and corrupted entries, all the way to failed line of business applications that depend on specific objects that must exist in the configuration container.	Specialized procedures used by the State of Washington make specific changes to configuration objects and ACLs, bypassing standard tools. This increases the likelihood that such a threat is realized.

Vulnerabilities

None identified.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Default permissions are set on the configuration container object as follows: ▪ "Full control" to "Domain Administrators" and System ▪ "Read" to "Authenticated Users" ▪ "Replication Synchronize" and "Manage Replication	The default permissions provide reasonable assurance that only members of the authorized groups listed on the left gain access to the settings and properties of objects in the configuration container. These permissions also enable domain controllers

Topology" to the "Enterprise Domain Controllers" group ▪ "Replication Synchronize" and "Manage Replication Topology" to the Builtin "Administrators" group ▪ "Enable Inheritable Full Control" to the "Enterprise Administrators" group ▪ "Enable Inheritable Auditing" to the Writes by Everyone	in the forest to replicate from each other and automatically, delaying the latency period and ensure exclusive control of the configuration container to the Enterprise Administrators group.

Constraints

None identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

Access to objects in the Active Directory configuration container will be restricted to members of the enterprise administrators group. Changes to permissions, creation of additional objects, and deletions of objects will be conducted only through formal procedures that are supported by Microsoft Product Support Services.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
No procedures required.	See "Change Management Document" for more information about submitting a change to the default permissions on configuration container objects.

Asset: Active Directory Schema

Description: The schema contains definitions for the universe of objects that can be stored in the directory, and it enforces the rules that govern both the structure and the content of the directory. The schema consists of a set of classes, attributes, and syntaxes that represent an instance of one or more classes in the schema.

Dependencies, Exposure and Value

Schema exposure is high because several applications, including Exchange Server 2000, require schema extensions before they can be installed on the system. Because only one schema exists per Active Directory Forest, the needs of all Washington State Agencies must be accommodated by it. Once deployed in production, the schema is probably the second most valuable asset in the forest, outside the objects and attributes defined by it.

Threats

For each threat identified, the table describes the threat agent and source (accidental or deliberate). The impact column describes the consequence and severity of a realized threat.

Description	Agent	Impact	Likelihood
Improper modification of schema classes, attributes, or syntaxes.	Internal Accidental or Deliberate	Impact ranges from minor inconveniences and corrupted entries, all the way to failed line of business applications that depend on specific objects that must exist in the schema. Additions to the schema can never be reversed, only disabled.	Moderate

Vulnerabilities

None identified.

Security Safeguards

The following safeguards can be implemented to reduce overall risk. The following table represents a list of available options and their impact on prevention, transfer of risk, reduction in the likelihood or vulnerability, mitigation or detection. The impact column also defines how implementing the safeguard contributes to the overall security goals of availability, integrity and confidentiality. Safeguards are used in conjunction with constraints to ultimately determine policies and procedures.

Safeguard	Impact
Windows 2000 limits access to the schema to members of the Schema Admins Enterprise Group.	This reduces the likelihood that, out of the box, Windows 2000 will allow unauthorized users to make schema modifications.
Windows 2000 does not publish schema modification tools in the default administrator interface.	This requires administrators to seek out information about modifying the schema and ensures, at least to a

	small degree, that administrators understand the implications of their actions before making changes to the schema.

Constraints

None identified.

Policy

Based on the assessment of threats, vulnerabilities, available safeguards, and constraints, the following security policy is to be implemented on the State of Washington Windows 2000 Forest.

Objective

The Active Directory Schema is owned and maintained by the Enterprise Schema Administrators group. All changes to the Schema must be submitted through the change management process with a valid business justification and approved by the Forest Resource Group and Forest Steering Committee.

Procedures

The policy defined above will be implemented as follows:

Description	Step-by-Step Instructions
All changes must be submitted and approved through the change management process.	See "Change Management Document" for more information about submitting and approving changes.

Forest-Wide Security Policies

In addition to the specific control procedures identified in each of the preceding sections, several forest-wide controls are in place to ensure proper security of Windows 2000 assets. The policies and procedures are grouped in categories, referred to as general controls. It is the responsibility of all agencies to ensure that these general controls are observed in each child domain.

These policies represent the minimum requirements as defined by the forest resource group to ensure security and recoverability of the Statewide Forest. Most agencies will require additional security procedures not defined here to meet their own requirements for security.

Authentication – Domain Administrators

- All Domain Administration Account login IDs must be authorized and approved.
- All Domain Administrator accounts are to be used for administration purposes only. Each Administrator will have a normal user account for day-to-day office work.
- All Domain Administration Account login IDs must have a complex password of at least 8 characters. Complexity is defined as having at least three of the following four types of characters: lower case letters, upper case letters, numbers, or special character.
- Login IDs are not to be shared.
- Only the owner of a password is to know that password.
- Passwords must be changed every 90 days. Passwords cannot be changed for at least 7 days after the initial change (minimum password change length).
- System lockout will take effect for 30 minutes if more than 5 bad login attempts are made within a 30 minute period.
- Password history is maintained for 18 iterations, ensuring that the same password is not re-used at least 18 times.

Authentication – Users

1. Must follow ISB Recommendations for General Access Security

Authorization (Access Controls)

1. Groups are used to manage permissions to all Active Directory Objects, including file shares and printers.
2. Use Secure Dynamic Updates for Dynamic DNS entries.
3. Use Organizational Units to group users and administrators, applying the appropriate policies to each.
4. Set permissions compatible with Windows 2000 Only (non mixed-mode).
5. Domain controllers are physically secured.

Audit

1. Each agency must define and maintain an intrusion detection policy. At a minimum, intrusion detection should regularly monitor failed login attempts.
2. Changes made to the security policy of a domain must be audited.

Backup and Recovery

1. Each agency is responsible for maintaining at least two iterations of validated backup information for the active directory data in their domain (to ensure recoverability of the state-wide global catalog)[2].
2. The media for validated domain backups must allow a recovery history of at least 30 days and must be stored off-site.
3. All backup media, on and off-site, must be securely stored.

[2] Two iterations and 30 days of history are a minimum. The purpose behind multiple iterations is to allow for the possibility that the most recent backup information is corrupt or invalid. The purpose behind the 30 day minimum is to ensure that the state can recover from any problem that may have been discovered during the past month.

Appendix A – Forest Wide Asset List

The following table serves as a reference for all assets identified for protection in the State of Washington Forest Security Plan.

ASSET	DESCRIPTION
DNS Topology Information	The topology of the DNS infrastructure should be prevented from exposure to external users. Knowledge of such information allows unauthorized users to launch denial of service attacks or confidentiality breaches of specific servers. DNS must also be protected from unauthorized personnel making changes to the DNS database resource records.
WINS Database	The WINS database is an alternative to DNS for name resolution of legacy clients, servers, and services. It must be protected from unauthorized changes and loss of use.
Active Directory Global Catalog	The Global Catalog is a complete list of all objects in the Active Directory environment. Every object is defined by attributes and the integrity of these attribute values is at risk. Object data must be available to legitimate users, hidden from unauthorized users, and protected from change, except by appropriate state personnel.
AD Replication Traffic	Protection of the Global Catalog must be preserved during replication across WAN and domain boundaries. Traffic must be protected from unauthorized "listening" or monitoring by unauthorized users.
FSMO Roles	The FSMO roles in the root domain and forest contain information that is vital to the ongoing maintenance, support and expansion of Active Directory. The FSMO roles must remain available and should be protected from compromise.
Active Directory Schema	The schema contains class and attribute definitions for objects in Active Directory and within Global Catalog servers. It must be protected from unauthorized changes and loss of use.
Active Directory Configuration Partition	This describes the logical structure of your deployment, containing information such as domain structure or replication topology. It must be protected from unauthorized change an loss of use.
Root Hardware and System Resources	Because the hardware ultimately houses the active directory environment, it must be protected from unauthorized access, tampering, or change.

Appendix B – Forest Wide Threats

The following table provides a summary of all identified threats, the agents that can carry out those threats, assets affected and an analysis of the likelihood of each threat occurring.

THREAT	AGENT(S)	ASSETS AFFECTED	IMPACT
Loss	Theft or destruction by External or Internal Person Accidental Failures	Domain Controllers Agency-specific Resources Email Systems	Minimal to Severe, depending on criticality of data
Corruption	Unauthorized Changes or Operator Error by Internal or External Person	Active Directory Schema DNS Infrastructure Global Catalog Data Users, Groups and Policies FSMO Roles Root Hardware	Moderate to Severe
Insufficient Resources	Accidental Failures	Hardware Resources Human (Operations) Resources	Minimal to Moderate
Compromise	Theft or Accidental Disclosure	Global Catalog Data DNS Infrastructure Agency Resources	Moderate to Severe
Loss of Access	Denial of Service (Internal or External) Accidental Failures	All assets and resources subjected.	Minimal to Severe

References

[1] Hutt, Bosworth and Hoyt, Computer Security Handbook, Third Edition. "Information Security Risk Management," 1995, page 3·1.
[2] *ibid*, page 3·5.
[3] *ibid*, page 3·11.
[4] *ibid,* page 3·12.
[5] Sanderson and Rice, Guide to Securing Microsoft Windows 2000 Active Directory (NSA). 2000, Page 6.
[6] Stephens, Guide to Securing Microsoft Windows 2000 DNS (NSA). 2001, Page 6.
[7] *5 ibid*, Page 6.